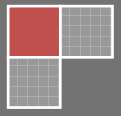
Taxonomic Modeling of Security Threats in Software Defined Networking

Recent advances in software defined networking (SDN) provide an opportunity to create flexible and secure next-generation networks. Many companies have expressed the interest in SDN utilization. Although much has been said about the ability of SDN to solve persistent network security problems, our current knowledge on SDN vulnerabilities, threats, and attacks is limited. In this paper, I use the threat modeling approach to develop a novel SDN threat model that provides a foundation for identifying possible threats to SDNs.

Jennia Hizver, PhD
BlackHat Conference
August 5-6, 2015



Contents

1 Introduction

Software Define Networking (SDN) is an emerging networking paradigm that aims to change the limitations of the traditional networking. The value of SDN lies in its ability to provide consistent policy enforcement and deliver greater scalability and control over the entire network by means of centralized management and network programmability. The next generation of security solutions will take advantage of the wealth of network usage information available in SDN to improve policy enforcement and traffic anomaly detection and mitigation.

Although much has been said about the benefits of SDN to solve persistent network security problems, our current knowledge on SDN threats and attacks is limited. The new systems required to carry out SDN functions may themselves come under malicious attacks. While some attacks will be common to existing networks, others will be more specific to SDN. Adversaries will inevitably exploit SDN systems if a successful network compromise could be achieved through such exploitations. A vulnerable SDN network could therefore undermine security and availability of the entire network.

In order to secure SDN networks, all of the potential security threats and attacks must be anticipated before attackers take advantage of vulnerabilities. In this paper, I describe a novel SDN threat model, which looks at SDN from an adversary's perspective to identify potential threats to and attacks on SDN at the architectural level, regardless of whether or not these threats can be successfully carried out. I further apply the threat model to synthesize a set of potential real-life attacks adversaries could launch against SDN networks. Finally, I provide security recommendations to address the threats.

2 SDN Attack Surface

The SDN threat modeling requires understanding of the SDN architectural components and their interconnections. Figure 1 illustrates a typical SDN architecture to reveal the main SDN building blocks, which include the SDN planes and interfaces. Any of these architectural components could contain vulnerabilities and be exploited by attackers to compromise a SDN network. The overall SDN attack surface is represented by the sum of all of these components.

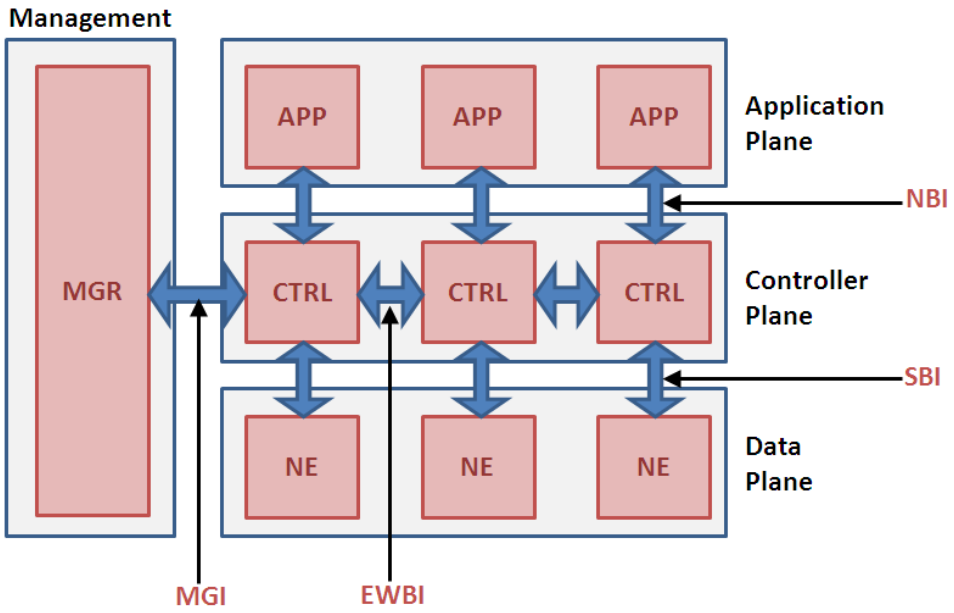


Figure 1. The SDN components include applications (APP), controllers (CTRL), network elements (NE), management consoles (MGR), the northbound interface (NBI), the southbound interface (SBI), east/west bound interface (EWBI), and the management interface (MGI).

The following planes are identified in SDN:

- the data plane comprising network elements for traffic forwarding or processing
- the controller plane comprising a set of controllers, which control network elements in the data plane
- the application plane comprising applications with access to resources exposed by controllers
- the management plane comprising management consoles for applications, controllers, and network elements and supporting remote management tasks.

The following interfaces are identified in SDN:

- the east/west bound interfaces required by distributed controllers for importing/exporting data between controllers and monitoring/notification capabilities
- the northbound interfaces enabling the communication between the controller plane and the application plane

- the southbound interfaces providing the link between the controller plane and the data plane
- management interfaces performing management functions on applications, controllers, and network elements in each plane.

3 SDN Threat Model

In order to systematically identify threats affecting SDN, I decompose each threat into 3 elements:

- threat source – a source triggering the vulnerability
- vulnerability source – a SDN component where the vulnerability arises
- threat action – an action by which the threat is carried out

I classify the threat sources into the following (see Figure 2):

- a non-SDN component – system that is not a part of the SDN architecture
- a rogue SDN component – an unauthorized SDN system within a SDN network engaged in unauthorized activities
- a malicious SDN application (a compromised application or a user engaged in malicious activities using the application)
- a malicious controller (a compromised controller or a user engaged in malicious activities on the controller)
- a malicious network element (a compromised network element or a user engaged in malicious activities using the network element)
- a malicious management console (a compromised management console or a user engaged in malicious activities using the console)